



# Qualys Cloud Platform (VM, PC) v8.x

## Release Notes

Version 8.21.2

September 18, 2019

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

### **Qualys Cloud Platform**

[Virtual Scanner Appliance Support for Alibaba Platform](#)

### **Qualys Vulnerability Management (VM)**

[Schedule an EC2 Scan with no scannable EC2 Assets in Asset Tags](#)

### **Qualys Policy Compliance (PC)**

[Expanded Support for Instance Discovery & Auto Record Creation](#)

[Oracle 19c Support](#)

[Scan Results Shown for SUSE 11.x from Cloud Agent Scans](#)

[Added Ubuntu 14.x and SUSE 12.x to the Unix Directory Check UDC](#)

[New Technologies Supported in Compliance Scans for Unix Hosts](#)

[Support for New OCA Technologies](#)

[View History of Control Status Changes](#)

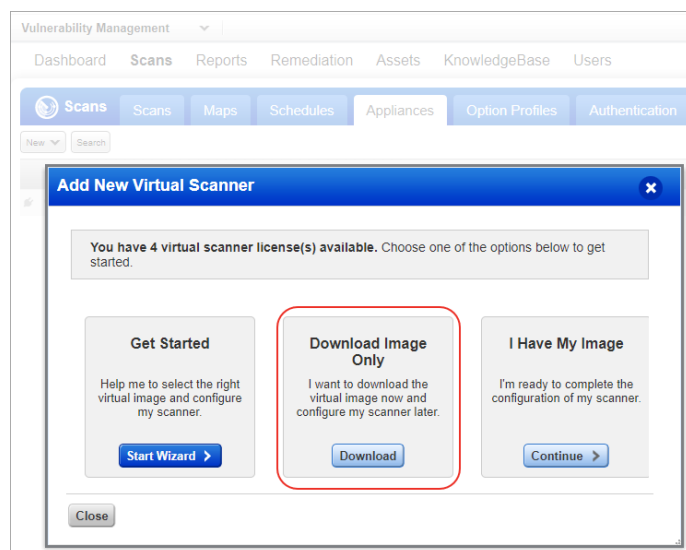
[Support for Red Hat Fedora 30](#)

**Qualys 8.21.2 brings you many more improvements and updates! [Learn more](#)**

# Qualys Cloud Platform

## Virtual Scanner Appliance Support for Alibaba Platform

We now support Qualys Virtual Scanner Appliance for Alibaba Cloud Compute.



To download virtual scanner images from the Qualys UI, go to New >Virtual Scanner.

Then click Download under "Download Image Only".

Qualys Virtual Scanner Appliance			
Available Distributions			
Overview			
The Qualys Virtual Scanner Appliance has multiple distributions to support deployments on a variety of virtualization platforms. A virtual scanner license may be used to activate any of the below images.			
Distribution Package	Target Platforms	File/Package Type	File Location
Standard	<ul style="list-style-type: none"><li>VMware vSphere: vCenter Server, ESXi</li><li>VMware Workstation, Workstation Player, Fusion</li><li>Citrix XenServer</li></ul>	OVA with VMDK virtual disk format	<a href="#">Download</a>
OpenStack	<ul style="list-style-type: none"><li>OpenStack Newton</li></ul>	OVA with VMDK virtual disk format	<a href="#">Download</a>
VMware vApp	<ul style="list-style-type: none"><li>VMware vSphere: vCenter Server</li></ul>	VMware vApp OVA with VMDK virtual disk format <a href="#">(see note below)</a>	<a href="#">Download</a>
Microsoft Hyper-V	<ul style="list-style-type: none"><li>Microsoft Windows Server</li></ul>	ZIP with VHD virtual disk format	<a href="#">Download</a>
Amazon HVM Machine Image (Pre-Authorized Scanning)	<ul style="list-style-type: none"><li>Amazon EC2-Classic, Amazon EC2-VPC</li></ul>	AMI <a href="#">(see note below)</a>	<a href="#">AWS Marketplace</a>
Amazon HVM Machine Image	<ul style="list-style-type: none"><li>Amazon EC2-Classic, Amazon EC2-VPC</li></ul>	AMI <a href="#">(see note below)</a>	<a href="#">AWS Marketplace</a>
Microsoft Azure Marketplace Image	<ul style="list-style-type: none"><li>Microsoft Azure Cloud Platform</li></ul>	VHD	<a href="#">Azure Marketplace</a>
Google Compute Cloud Image	<ul style="list-style-type: none"><li>Google Cloud Platform</li></ul>	Google Compute Engine Image	<a href="#">Google Cloud Launcher</a>
Oracle Cloud Marketplace Image	<ul style="list-style-type: none"><li>OCI and OCI-Classic</li></ul>	Oracle Cloud Compute Image	<a href="#">OCI in Marketplace</a> <a href="#">OCI-Classic in Marketplace</a>
Alibaba Cloud Marketplace Image	<ul style="list-style-type: none"><li>Alibaba Cloud Compute</li></ul>	Alibaba ECS Image	<a href="#">Alibaba Marketplace</a>

You'll see the list of Available Distributions including the new Alibaba Marketplace Image.

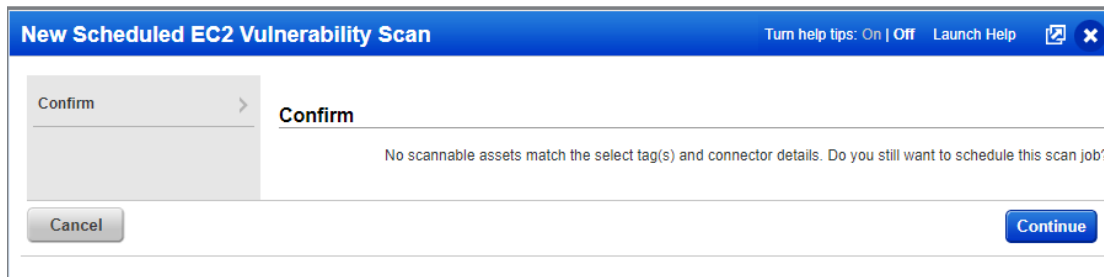
Follow the appropriate link to go directly to the Qualys Virtual Scanner Appliance page in the Alibaba Marketplace.

The distribution list screen on the left highlights the new distribution for Alibaba platform.

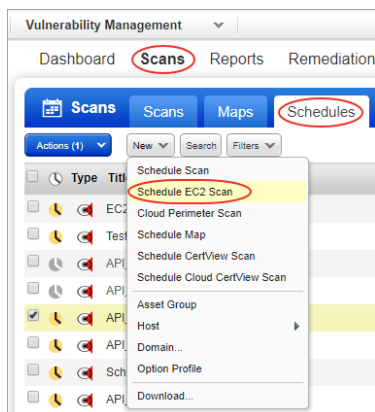
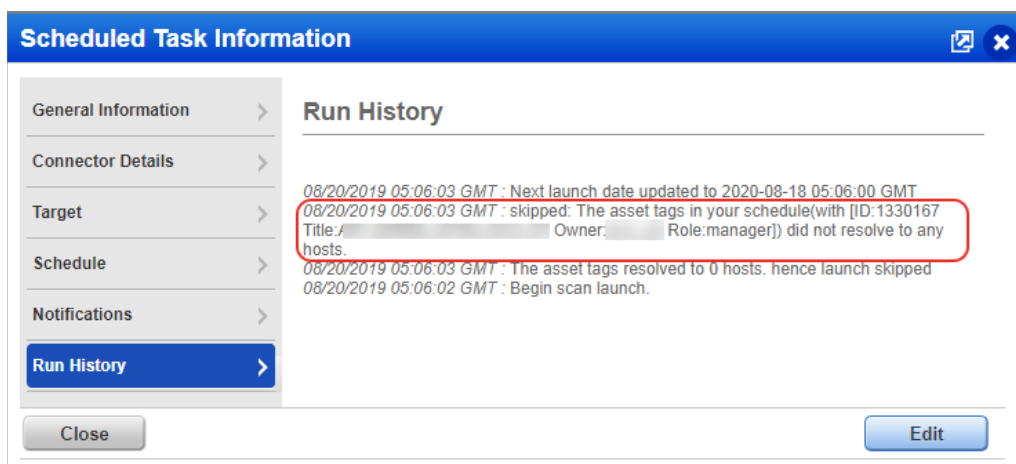
## Qualys Vulnerability Management (VM)

### Schedule an EC2 Scan with no scannable EC2 Assets in Asset Tags

An account Manager or Unit Manager can schedule an EC2 scan even if at the time of scheduling, the tags don't resolve to hosts in your account. This way you can schedule the scan and if new hosts show up later that match the asset tags then they'll be scanned automatically as per the schedule. When you schedule an EC2 scan with such tags, the system will show you a message that "No scannable assets match the select tag(s) and connector details. Do you still want to schedule this scan job?".



If you choose Continue, the system will schedule a new EC2 scan for selected asset tags. During the scan, scanning will be skipped for the asset tags with no scannable assets. After the scan, if you open the scheduled task in the "Info" mode and go to the "Run History" tab, you will see that the scan is skipped for asset tags that don't resolve to hosts.



Not sure how to schedule an EC2 scan? It's easy.

To schedule an EC2 scan, go to Scans > Schedules and in the New menu select Schedule EC2 Scan.

# Qualys Policy Compliance (PC)

## Expanded Support for Instance Discovery & Auto Record Creation

Instance discovery and auto record creation is now supported for IBM WebSphere App Server and Jboss Server. This was previously supported for Apache Web Server. You can learn more about this feature and how it works in the "System Authenticated Records" help file.

### Summary

These capabilities now are available for IBM WebSphere App Server and Jboss Server.

- Support for scanning multiple instances running on the same host, and when hosts have varying configurations
- 2 phased scanning process. First, a discovery scan finds IBM WebSphere/JBoss instances, consolidates instance data, and creates/updates auth records in the user's account. Then an assessment scan uses the records saved in the user's account for control evaluations.
- New option profile settings allow you to 1) enable instance discovery and auto record creation, 2) include system-created records for scans, and 3) determine whether to send system records or user records when there are 2 records for the same instance configuration.
- Compliance scan results show a list of instances discovered by the scan when the instance discovery and auto record creation feature is enabled for the scan. Compliance assessment data is not collected during instance discovery scans.
- New System created auth records. Auto created authentication records have the owner "System". These records cannot be edited by users.
- You can enable IBM WebSphere/JBoss records for authenticated scanning, i.e. set as Active, or disable this, i.e. set as Inactive.

### Option Profiles

When configuring option profiles you'll now see IBM WebSphere App Server and Jboss Server listed under System Authentication Records.

Option Profile 1: Choose "Allow instance discovery and system record creation" and select one or more application.

Use this option profile for instance discovery scans. We'll discover running instances during the scan, and then use the information collected about your running instances to create auth records.

For JBoss server, Unix and/or Windows authentication are required while for IBM

**System Authentication Records**

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. [Learn more about instance discovery and system authentication records](#)

**Create System Authentication Records**

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required. Compliance assessments will not be performed for any technology.

☒ Allow instance discovery and system record creation

For the following technology

☐ Apache Web Server

☒ IBM WebSphere App Server

☒ Jboss Server

**Use System Authentication Records**

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

☐ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

☒ User created record

☐ System created record

WebSphere server, only Unix authentication is required. So be sure you have Unix/Windows records in your account depending on the technology for which you want to discover instances.

Option Profile 2: Choose “Include system created authentication records in scans” in the option profile you’ll use for compliance assessments.

System created records will be used along with user created records. If you have a user created record and a system created record for the same instance configuration we’ll use the user record by default. You can change this if you prefer to use the system record.

**System Authentication Records**

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. [Learn more about instance discovery and system authentication records](#)

Create System Authentication Records

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required. Compliance assessments will not be performed for any technology.

☐ Allow instance discovery and system record creation  
For the following technology

☐ Apache Web Server  
☐ IBM WebSphere App Server  
☐ Jboss Server

**Use System Authentication Records**

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

☒ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

☒ User created record  
☐ System created record

## Compliance Scan Results

For a compliance scan with the option "Allow instance discovery and system record creation", you can go to the Appendix section of your compliance scan results to see the auto discovered instances.

Compliance Scan Results	
File ▾	Help ▾
Appendix	
Windows authentication was successful for these hosts	
10.10.36.111	
Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts	
10.10.26.46, 10.10.31.129, 10.10.34.52, 10.10.35.24, 10.10.35.241, 10.10.35.249, 10.11.70.44, 10.11.70.118	
Auto Discovered Instances	
IBM WebSphere App Server (Installation Directory: /opt/IBM/WebSphere3/AppServer)	
10.10.35.24, 10.10.35.241	
IBM WebSphere App Server (Installation Directory: /opt/IBM/WebSphere/AppServer)	
10.10.34.52, 10.10.35.24	
Jboss Server (Root Directory: /opt/wildfly11_2, Base Directory: /opt/wildfly11_2/standalone, Base Config Directory: /opt/wildfly11_2/standalone/configuration, Config File Path: /opt/wildfly11_2/standalone/configuration/standalone.xml, Mode: Standalone)	
10.11.70.44	
Jboss Server (Root Directory: /opt/wildfly11_1, Base Directory: /opt/wildfly11_1/standalone, Base Config Directory: /opt/wildfly11_1/standalone/configuration, Config File Path: /opt/wildfly11_1/standalone/configuration/standalone.xml, Mode: Standalone)	
10.11.70.44	


In the following example we didn't find running instances for scanned hosts.

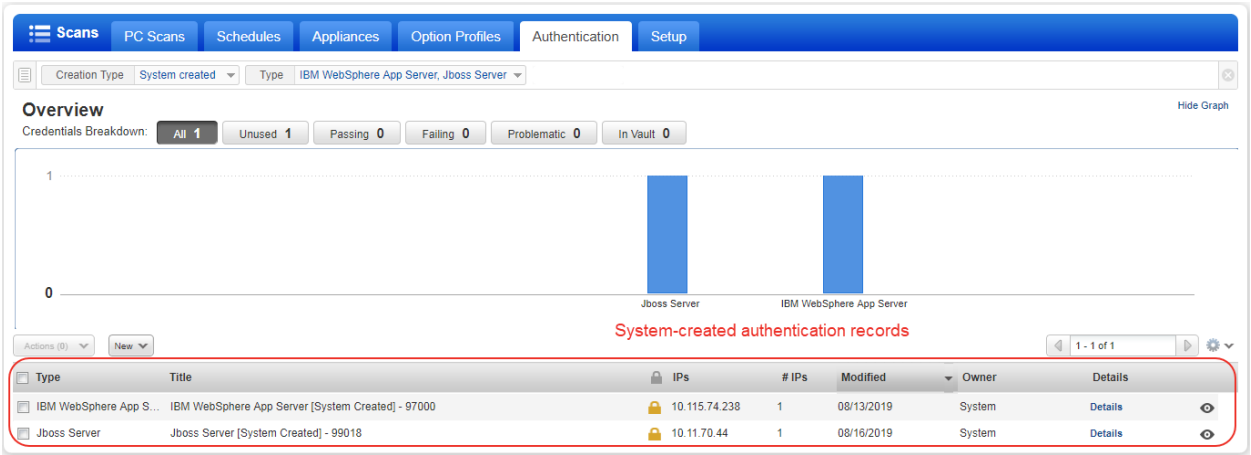
Compliance Scan Results	
File ▾	Help ▾
<b>Appendix</b>	
<b>Target hosts found alive (IP)</b>	
10.10.26.134	
<b>Target distribution across scanner appliances</b>	
qvs_a_ashrestha : 10.10.26.134	
<b>Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts</b>	
10.10.26.134	
<b>Auto Discovered Instances</b>	
<b>IBM WebSphere App Server instances were not found for these hosts</b>	
10.10.26.134	
<b>Jboss Server instances were not found for these hosts</b>	
10.10.26.134	

In this case we didn't find the authentication type on any scanned hosts.

Compliance Scan Results	
File ▾	Help ▾
<b>Appendix</b>	
<b>Target hosts found alive (IP)</b>	
10.10.26.134	
<b>Target distribution across scanner appliances</b>	
qvs_a_ashrestha : 10.10.26.134	
<b>Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts</b>	
10.10.26.134	
<b>Auto Discovered Instances</b>	
<b>IBM WebSphere App Server instances were not found for these hosts</b>	
10.10.26.134	
<b>Jboss Server instances were not found for these hosts</b>	
10.10.26.134	
<b>Authentication record instance information was not collected for the following types</b>	
Apache Web Server	

System Created Records

You'll see a gold lock  and Owner "System" for system-created authentication records for IBM WebSphere App Server and Jboss Server.



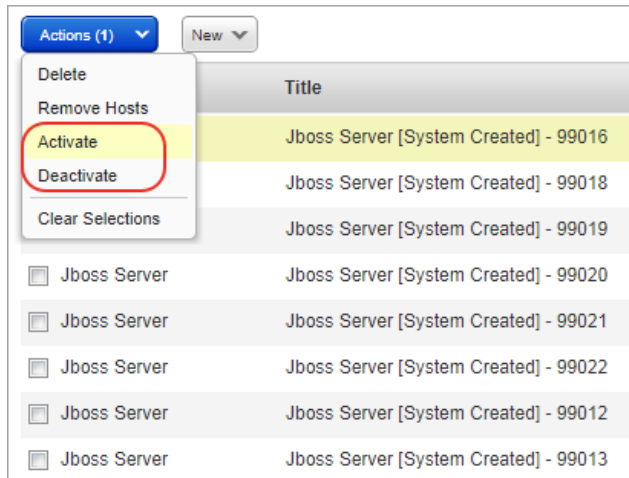
Also, when you download the authentication records list to CSV format (New > Download) you'll see the column "Is System Created" with a value of Yes or No for each record.

Network	Type	Title	Is System Created	IPs	IPs	Modified	Owner	Status
Global Defa	IBM WebSphere App Server	IBM WebSphere App Server [System Created] - 103007	Yes	10.10.34.5	2	08/21/2019 at 1	System	Active
Global Defa	IBM WebSphere App Server	IBM WebSphere App Server [System Created] - 103009	Yes	10.10.35.2	2	08/21/2019 at 1	System	Active
Global Defa	IBM WebSphere App Server	IBM WebSphere App Server [System Created] - 103010	Yes	10.10.35.2	1	08/21/2019 at 1	System	Active
Global Defa	IBM WebSphere App Server	IBM WebSphere App Server [System Created] - 103011	Yes	10.10.35.2	1	08/21/2019 at 1	System	Active
Global Defa	IBM WebSphere App Server	IBM WebSphere App Server [System Created] - 103012	Yes	10.10.35.2	1	08/21/2019 at 1	System	Active

Type	Title	Is System Created	IPs	IPs	Modified	Owner	Status
Jboss Server	Jboss_unix3	No	10.115.68.152	1	08/21/201	Prerna T (N	Active
Jboss Server	Jboss_unix2	No	10.115.68.152	1	08/21/201	Prerna T (N	Active
Jboss Server	Jboss Server [System Created] - 102000	Yes	10.10.36.111	1	08/21/201	System	Active
Jboss Server	Jboss Server [System Created] - 102001	Yes	10.10.36.111	1	08/21/201	System	Active
Jboss Server	Jboss Server [System Created] - 102002	Yes	10.10.36.111	1	08/21/201	System	Active
Jboss Server	Jboss Server [System Created] - 102003	Yes	10.10.36.111	1	08/21/201	System	Active
Jboss Server	Jboss Server [System Created] - 102004	Yes	10.10.36.111	1	08/21/201	System	Active
Jboss Server	Jboss Server [System Created] - 102006	Yes	10.11.70.44	1	08/21/201	System	Active

## Make Records Inactive

Now you can make any IBM WebSphere App Server or Jboss Server authentication record inactive. This is already supported for Apache Web Server. Inactive records are not included in scans (even if the "Include system created authentication records in scans" option is selected in the option profile). Simply choose the records you want to make Inactive and pick Deactivate from the Actions menu above the data list. To activate records choose Activate.



## Want to know more?

Search the help for "System Authentication Records". For details on API changes, please see the Qualys API Release Notes.



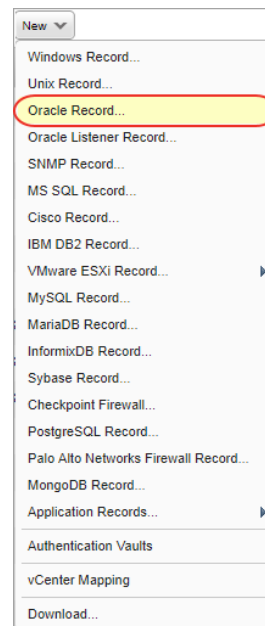
## Oracle 19c Support

We've extended our support for Oracle authentication to include Oracle 19c. We already support Oracle 11g, 12c, 18c, 9i.

You'll need a Oracle authentication record to authenticate to an Oracle database instance running on a Unix or Windows host, and scan it for compliance. For authentication to Windows hosts, enter the Windows file. For authentication to Unix hosts, enter the Unix file. You may enter one or both.

### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Unix or Windows record already defined for the host running the database.
- Create an Oracle record for the same host. Go to New > Oracle Record.



### Sample Reports

You'll see the Oracle 19c host technology in compliance reports and in compliance scan results.

**Compliance Scan Results**  
File ▾ Help ▾  
Title: INSTA  
Asset Groups: Oracle  
IPs: 10.11.7  
Excluded IPs: -  
Compliance Profile: Initial F

**Appendix**  
**Target hosts found alive (IP)**  
10.11.70.182  
**Target distribution across scanner appliances**  
vs\_seenu\_ak-2 : 10.11.70.182  
**Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts**  
10.11.70.182  
**Oracle authentication was successful for these hosts**  
Port 1527, SID ora19csu:  
10.11.70.182

**Results**  
10.11.70.182 2 of 2 (100%)  
**Unix/Cisco/Checkpoint Firewall**

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE
10.11.70.182 (-, -)	Oracle Enterprise Linux 7.x		Passed	-

  
**Oracle**

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE
10.11.70.182 (-, -)	Oracle 19c	Port=1527, SID=ora19csu	Passed	-

## Policies and Controls

You'll see Oracle 19c in the technologies list when creating a new policy.

**Create a New Policy**

**Empty Policy:** Build your policy from scratch.  
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

**Technologies** Select at least one technology. REQUIRED

Search technologies:  Add All | Remove All

No technologies selected 197 technologies Add all shown

- Oracle 12c
- Oracle 18c
- Oracle 19c**
- Oracle 9i
- Oracle Enterprise Linux 4.x
- Oracle Enterprise Linux 5.x
- Oracle Enterprise Linux 6.x

Back Choose Source Next

You'll see Oracle 19c when searching controls by technologies.

**Qualys Enterprise**

Policy Compliance Help Logout

Dashboard **Policies** Scans Reports Exceptions Assets Users

**Policies** Policies Controls Mandates Setup

1 - 500 of 11444

**Search**

CIDs:  Example: 1072,1071,1091 (up to 20)

Text:

Status: ☐ Deprecated

Technologies: ☐ Oracle 12c ☐ Oracle 18c ☒ **Oracle 19c** ☐ Oracle 9i ☐ Oracle Enterprise Linux 4.x

Frameworks: ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0 ☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manage ☐ CCI List 1 ☐ CIS - Apache HTTP Server 2.2 Benchmark v3.4.0 (09-23-20)

Framework ID:

Search

**Find controls for this technology**

## Scan Results Shown for SUSE 11.x from Cloud Agent Scans

With this release, you'll also get scan results for SUSE 11.x from cloud agent scans if the technology is selected in the UDC. This applies to all Unix UDCs. Prior to this release, you wouldn't get results from cloud agent scans even if the technology was selected in the UDC. Only compliance scans using scanners would return results for SUSE 11.x.

## Added Ubuntu 14.x and SUSE 12.x to the Unix Directory Check UDC

We now support 2 new technologies Ubuntu 14.x and SUSE 12.x in the Unix Directory Check UDC. These technologies were already supported in other Unix UDCs for scans using scanners. These technologies are also now supported by agent scans for all Unix UDCs. They weren't supported by agent scans before.

## New Technologies Supported in Compliance Scans for Unix Hosts

We now support 2 new host technologies "Elasticsearch" and "Apache Kafka" in compliance scans for hosts running on Unix platform. Elasticsearch and Apache Kafka information appears for scanned hosts in Compliance scan reports and Authentication reports when the applications are found on the scanned hosts.

You'll need a Unix authentication record for the hosts running Elasticsearch and Apache Kafka. Then scan those hosts using authentication.

### Sample Reports

Sample reports show Elasticsearch host technology in Authentication report and compliance scan results for a Unix host.

### Appendix

#### Targets with OS authentication-based technologies

10.115.98.210 (-, -)

Network: Global Default Network    Last Auth: 08/05/2019 at 12:03:57 PM (GMT+0530)  
OS: CentOS Linux 7.2.1511    Last Success: 08/05/2019 at 12:03:57 PM (GMT+0530)

S.N.	Host Technology	Instance
1	Elasticsearch	Elasticsearch (Binary Path: /etc/elasticsearch)

### Compliance Scan Results

File ▾   Help ▾

#### Appendix

Target hosts found alive (IP)  
10.115.98.210

Target distribution across scanner appliances  
VirtualIndiaScanner-1 : 10.115.98.210

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts  
10.115.98.210

Application technologies found based on OS-level authentication

Elasticsearch was found for these hosts  
Elasticsearch (Binary Path: /etc/elasticsearch)  
10.115.98.210

Compliance Profile:

Initial Profile

Scan Settings

Scan Restriction by Policy    Disabled

Auto Update Expected Value    -

Sample reports show Apache Kafka host technology in Authentication report and compliance scan results for a Unix host.

### Appendix

#### Targets with OS authentication-based technologies

10.115.98.186 (-, -)

Network: Global Default Network    Last Auth: 07/24/2019 at 01:59:38 PM (GMT+0530)  
OS: CentOS Linux 7.3.1611    Last Success: 07/24/2019 at 01:59:38 PM (GMT+0530)  
apache kafka auth report - 20190724

S.N.	Host Technology	Instance
1	Apache Kafka	Apache Kafka (Kafka Configuration File: /opt/kafka_2.12-2.3.0/config/server.properties)
2	Internet Explorer 11	Internet Explorer 11

### Compliance Scan Results

File ▾ Help ▾

**Target distribution across scanner appliances**  
qvs\_a\_shrestha : 10.11.70.43-10.11.70.44,10.11.70.144

**MongoDB authentication failed for these hosts**  
MongoDB (Port: 27017, Database: admin)  
10.11.70.44

**Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts**  
10.11.70.43-10.11.70.44, 10.11.70.144

**Oracle WebLogic Server authentication was successful for these hosts**  
WebLogic 12 (Domain Path: /opt/Oracle/Middleware/Oracle\_Home/user\_projects/domains/base\_domain)  
10.11.70.43

**Application technologies found based on OS-level authentication**  
**Apache Kafka was found for these hosts**  
Apache Kafka (Kafka Configuration File: /kafka\_2.11-2.1.0/config/server.properties)  
10.11.70.44

## Support for New OCA Technologies

We now support the following new technologies on assets for which data is collected using Out-of-Band Configuration Assessment (OCA) tracking.

- Cisco FTD 6
- Cisco WLC 8

Simply, navigate to Reports tab and run the Policy Compliance Reports and Authentication Report on these technologies to view your compliance posture.

Sample: Authentication Report for Cisco FTD 6 and Cisco WLC 8

Cisco FDT Auth Report - 20190827

File ▾ View ▾ Help ▾

Cisco FTD

Host	Network	Host Technology	Instance	Status	Cause	OS	Last Auth	Last Success
13.13.1.2 (ashutosh02, TAN02TAN)	Global Default Network	Cisco FTD 6.x		Passed	-	Cisco FTD 6	08/21/2019	08/21/2019
Host	Network	Host Technology	Instance	Status	Cause	OS	Last Auth	Last Success

Cisco WLC

Host	Network	Host Technology	Instance	Status	Cause	OS	Last Auth	Last Success
13.13.1.3 (ashutosh04, TAN05TAN)	Global Default Network	Cisco WLC 8.x		Passed	-	Cisco WLC 8	08/21/2019	08/21/2019
Host	Network	Host Technology	Instance	Status	Cause	OS	Last Auth	Last Success

## View History of Control Status Changes

With this release you can view the scan dates when control status changes occurred. For a control with a status of Pass you'll see the first scan date when the control passed and the last scan date when the control passed. Similarly, for a control with a status of Fail you'll see the first and last scan date when the control failed. You'll see this on the Control View tab and in Policy Reports (depending on template settings).

### Good to Know

You must run new compliance scans with version 8.12.2 or later in order to view and report dates for control status changes.

You'll now see these control status details:

*Previous Status/Posture* - The compliance status (Pass or Fail) for each control prior to the most recent scan.

*First Fail Date* - The first scan date when the control was reported as Fail. If the previous status was Pass then this is the date the status changed from Pass to Fail.

*Last Fail Date* - The most recent scan date when the control was reported as Fail.

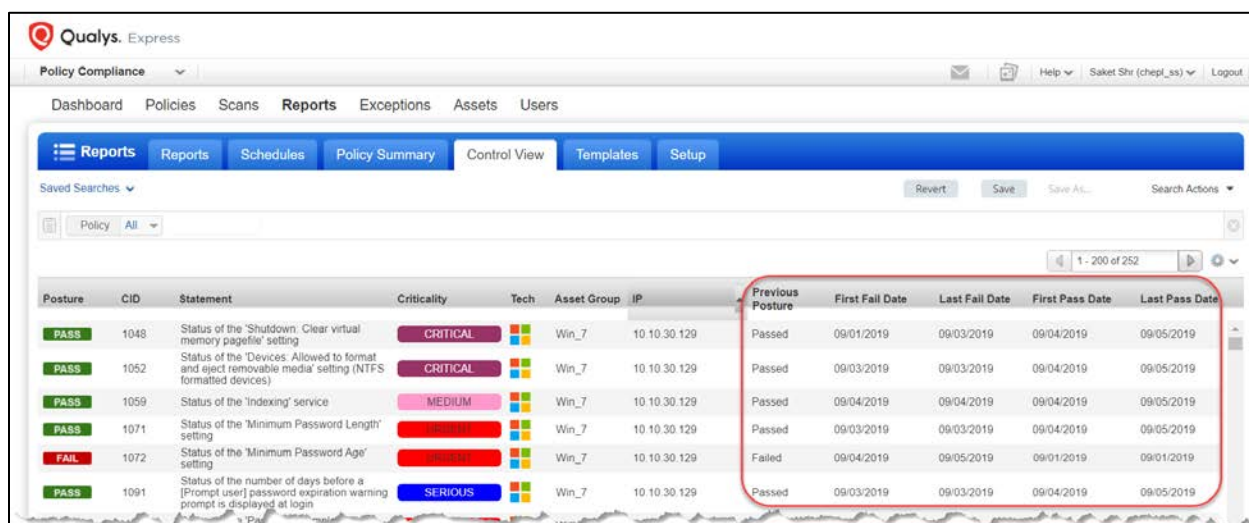
*First Pass Date* - The first scan date when the control was reported as Pass. If the previous status was Fail then this is the date the status changed from Fail to Pass.

*Last Pass Date* - The most recent scan date when the control was reported as Pass.

## Control View

New columns are added in Control View. Note - Records will be displayed in Control View only when there is some search criteria.

Go to PC > Reports > Control View. Enter search criteria and click Search to view controls in the list.

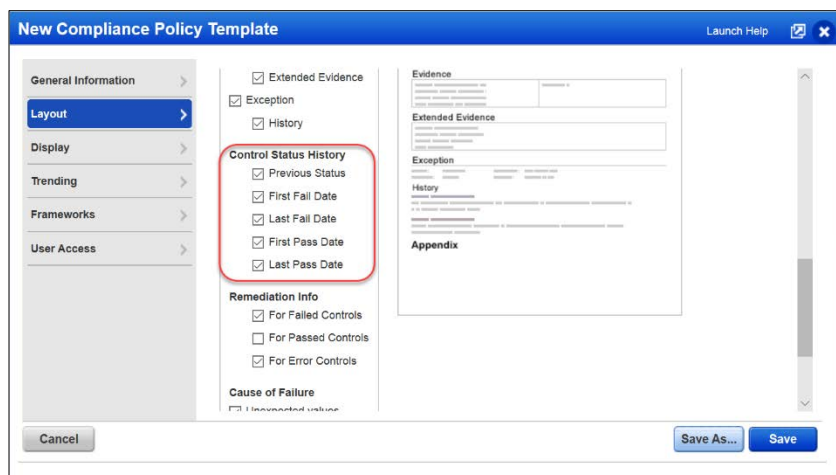


The screenshot shows the Qualys Express interface with the 'Control View' tab selected. A table displays control status changes with columns for Posture, CID, Statement, Criticality, Tech, Asset Group, IP, Previous Posture, First Fail Date, Last Fail Date, First Pass Date, and Last Pass Date. A red box highlights the last five columns.

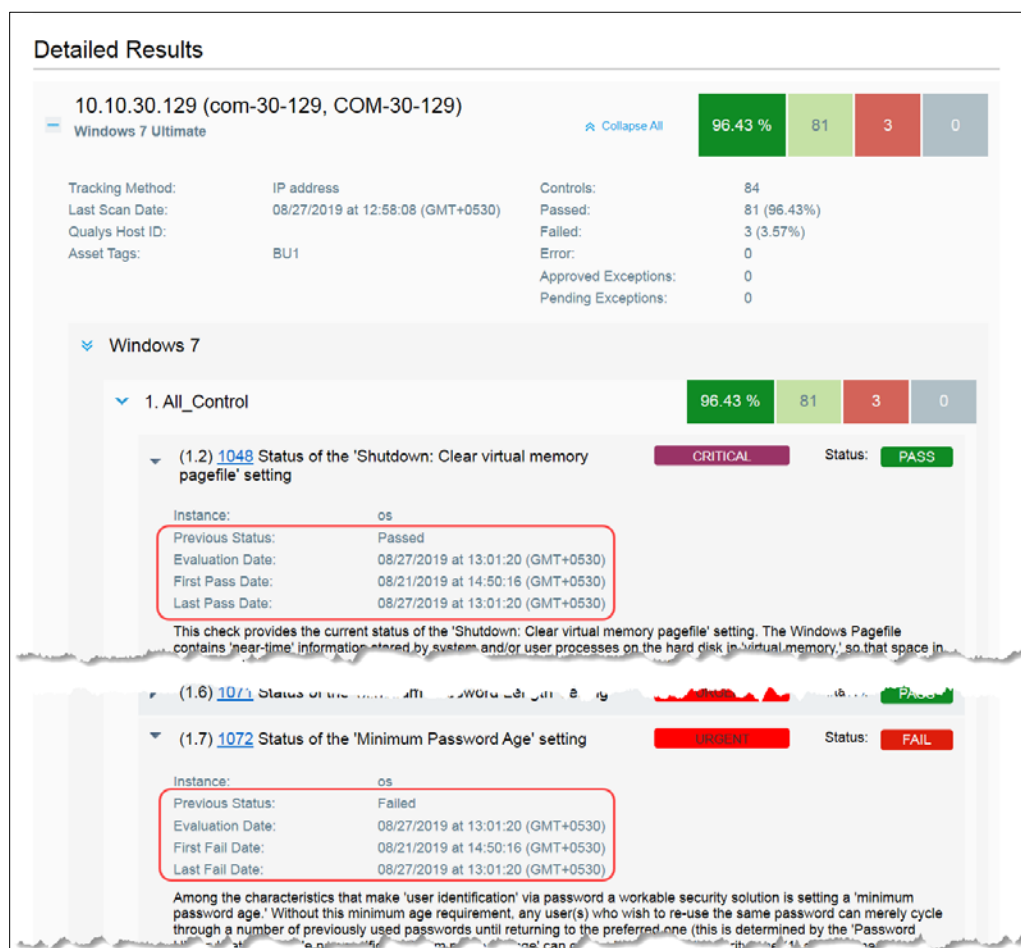
Posture	CID	Statement	Criticality	Tech	Asset Group	IP	Previous Posture	First Fail Date	Last Fail Date	First Pass Date	Last Pass Date
PASS	1048	Status of the 'Shutdown: Clear virtual memory pagefile' setting	CRITICAL	Win_7	Win_7	10.10.30.129	Passed	09/01/2019	09/03/2019	09/04/2019	09/05/2019
PASS	1052	Status of the 'Devices: Allowed to format and eject removable media' setting (NTFS formatted devices)	CRITICAL	Win_7	Win_7	10.10.30.129	Passed	09/03/2019	09/03/2019	09/04/2019	09/05/2019
PASS	1059	Status of the 'Indexing' service	MEDIUM	Win_7	Win_7	10.10.30.129	Passed	09/04/2019	09/04/2019	09/04/2019	09/05/2019
PASS	1071	Status of the 'Minimum Password Length' setting	CRITICAL	Win_7	Win_7	10.10.30.129	Passed	09/03/2019	09/03/2019	09/04/2019	09/05/2019
FAIL	1072	Status of the 'Minimum Password Age' setting	CRITICAL	Win_7	Win_7	10.10.30.129	Failed	09/04/2019	09/05/2019	09/01/2019	09/01/2019
PASS	1091	Status of the number of days before a [Prompt user] password expiration warning prompt is displayed at login	SERIOUS	Win_7	Win_7	10.10.30.129	Passed	09/03/2019	09/03/2019	09/04/2019	09/05/2019

## Policy Reports

You can now select new fields while creating a policy template and these fields will be displayed on reports. You can see the new fields in Policy Reports for all the output formats.



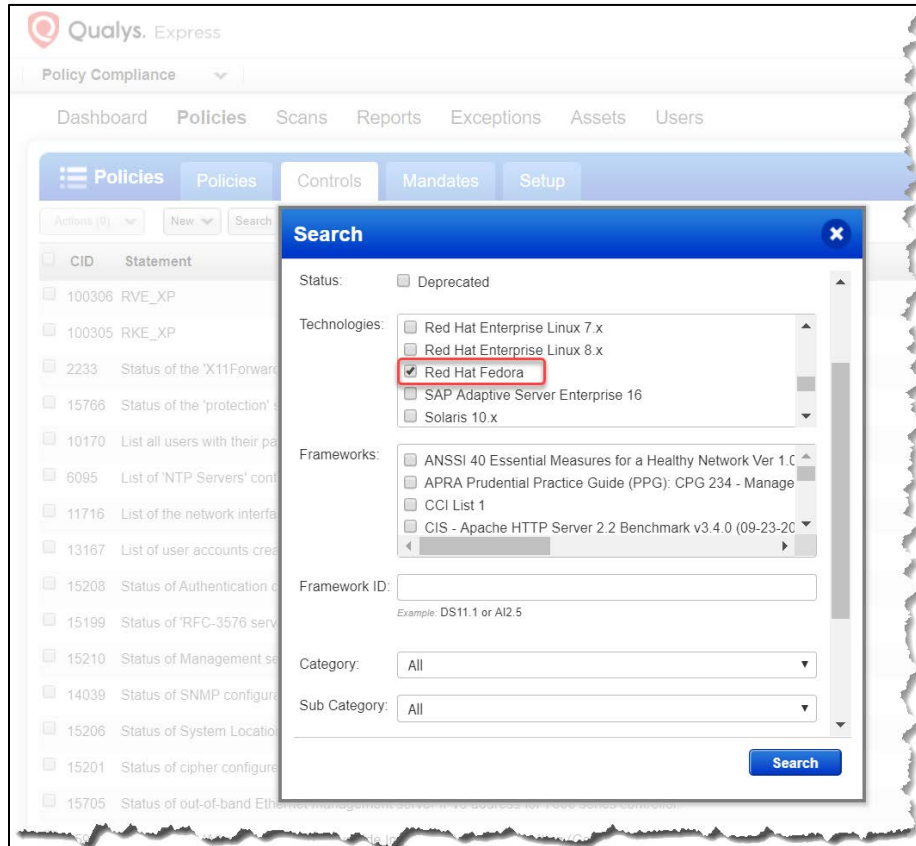
Go to Reports > Templates > New > Policy Template or edit an existing template. Make your selections on the Layout tab. In new policy templates, Previous Status is selected by default and you can select other fields.



Here's a sample Policy Report in HTML format. Expand control details to see control status history. The values shown depend on your report template selections and the current status of the control.

## Support for Red Hat Fedora 30

We've extended our support for Policy Compliance (PC) scan to include Red Hat Fedora 30. This new support is covered under existing technology name "Red Hat Fedora". We already support Red Hat Fedora 28 and Red Hat Fedora 29.





## Issues Addressed

- We fixed an issue where the next scheduled launch date for a scheduled scan with DST (daylight saving time) enabled was shown 1 day later than the actual next scheduled date. Now the next scheduled date is shown correctly for the scheduled scans.
- There was an issue where the IPs section which lists the scanned IP addresses was missing in the JSON output for the Scan API. The issue is now fixed, and the output lists all the IPs in the IPs section.
- We have fixed an issue and now the "Patch Published" dates in a patch report for all QIDs correctly show the dates in ISO 8601 format.
- We fixed an issue where creating/editing large policies were failing. As a result, controls were not shown for these policies. Now the policies show all the controls when created and updated.
- We fixed an issue where an incorrect expiration date was shown for the user account on activating a trial version of the Threat Protection module. Now we show a correct expiration date on activating or updating a trial version of Threat Protection module for the user account.
- The link to Help > Training will now redirect the User to Qualys Training page.
- We added help tips to better explain that while creating remediation tickets, rules with "Do not create tickets" action should be at the top of their rules list so they are applied first.
- To add some more clarity of how the superseded patches work we have added onscreen text for the "Exclude superseded patches" option in all report templates. We have also updated online help on using search lists and patch supersedence.
- The API User Guide is now updated to remove the "last" and "domain" input parameters for the Domain List API, as they are no longer used.
- We updated the API User Guide to add "include\_ignored" and "include\_disabled" parameters in the Detection Filters list for the Host list Detection API.